Contents

In-place Upgrades

3 minute read page test

The `istioctl upgrade` command performs an upgrade of Istio. Before performing the upgrade, it checks that the Istio installation meets the upgrade eligibility criteria. Also, it alerts the user if it detects any changes in the profile default values between Istio versions.

Canary Upgrade is safer than doing an in-place upgrade and is the recommended upgrade method.

The upgrade command can also perform a downgrade of Istio.

See the `istioctl upgrade reference` for all the options provided by the `istioctl upgrade` command.

`istioctl upgrade` is for in-place upgrade and not compatible with installations done with the `--revision` flag. Upgrades of such installations will fail with an error.

Upgrade prerequisites

Before you begin the upgrade process, check the following prerequisites:

- The installed Istio version is no more than one minor version less than the upgrade version. For example, 1.6.0 or higher is required before you start the upgrade process to 1.7.x.
- Your Istio installation was installed using istioctl.

Upgrade steps

Traffic disruption may occur during the upgrade process. To minimize the disruption, ensure that at least two replicas of `istiod` are running. Also, ensure

that `PodDisruptionBudgets` are configured with a minimum availability of 1.

The commands in this section should be run using the new version of `istioctl` which can be found in the `bin/` subdirectory of the downloaded package.

1. Download the new Istio release and change directory to the new release directory.
2. Ensure that your Kubernetes configuration points to the cluster to upgrade:

```
$ kubectl config view
```

3. Ensure that the upgrade is compatible with your environment.

```
$ istioctl x precheck
✔ No issues found when checking the cluster. Istio is safe to install
or upgrade!
To get started, check out https://istio.io/latest/docs/setup/getting-s
tarted/
```

4. Begin the upgrade by running this command:

```
$ istioctl upgrade
```

If you installed Istio using the `-f` flag, for example `istioctl install -f <IstioOperator-custom-resource-definition-file>`, then you must provide the same `-`

```
f flag value to the istioctl upgrade command.
```

If you installed Istio using `--set` flags, ensure that you pass the same `--set` flags to upgrade, otherwise the customizations done with `--set` will be reverted. For production use, the use of a configuration file instead of `--set` is recommended.

If you omit the `-f` flag, Istio upgrades using the default profile.

After performing several checks, `istioctl` will ask you to confirm whether to proceed.

5. `istioctl` will in-place upgrade the Istio control plane and gateways to the new version and indicate the completion

status.

6. After `istioctl` completes the upgrade, you must manually update the Istio data plane by restarting any pods with Istio sidecars:

```
$ kubectl rollout restart deployment
```

Downgrade prerequisites

Before you begin the downgrade process, check the following prerequisites:

- Your Istio installation was installed using istioctl.
- The Istio version you intend to downgrade to is no more than one minor version less than the installed Istio version. For example, you can downgrade to no lower than 1.6.0 from Istio 1.7.x.
- Downgrade must be done using the `istioctl` binary version that corresponds to the Istio version that you intend to downgrade to. For example, if you are downgrading from Istio 1.7 to 1.6.5, use `istioctl` version 1.6.5.

Steps to downgrade to a lower Istio version

You can use `istioctl upgrade` to downgrade to a lower version of Istio. The steps are identical to the upgrade process described in the previous section, only using the `istioctl` binary corresponding to the lower version (e.g., 1.6.5). When completed, Istio will be restored to the previously installed version.

Alternatively, `istioctl install` can be used to install an older version of the Istio control plane, but is not recommended because it does not perform any checks. For example, default values applied to the cluster for a configuration profile may change without warning.